(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 December 2000 (28.12.2000)

PCT

(10) International Publication Number
WO 00/79368 A1

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US00/17307

(22) International Filing Date: 21 June 2000 (21.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/338,915 23 June 1999 (23.06.1999) US

(71) Applicant: THE BRODIA GROUP [US/US]; Suite 1530, 221 Main Street, San Francisco, CA 94105 (US).

(72) Inventors: RUBIN, Paul; Suite 1530, 221 Main Street, San Francisco, CA 94105 (US). GOLDSTEIN, Theodore, Charles; Suite 1530, 221 Main Street, San Francisco, CA 94105 (US).

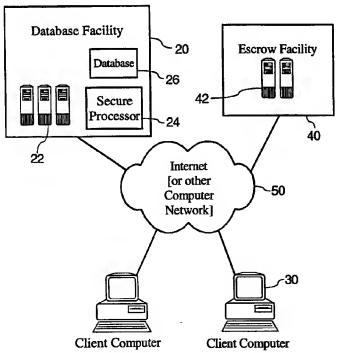
(74) Agent: MEYER, Virginia; Meyer Intellectual Property Law, Suite 275, 475 Gate Five Road, Sausalito, CA 94965 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SOFTWARE SMART CARD




(57) Abstract: Methods and systems for preventing unauthorized access to data stored on a computerized database (26). The present invention contemplates storing data corresponding to individual user accounts in encrypted form. The present invention involves two separate entities to accomplish a secure database (26): a database facility (20) and an escrow facility (40). The database facility (20) is in physical possession of and administers the database (26). According to the invention, data corresponding to an individual account is encrypted with a unique cryptographic key. The database facility (20), however, has no possession or knowledge of the cryptographic keys used to encrypt the data corresponding to individual user accounts. Rather, after the data is encrypted, the encryption key is transmitted to an escrow facility (40), which is independent from the database facility (20). Alternatively, the encryption key is itself encrypted and stored at the database facility (20) in a form that only the escrow facility (40) can readily decrypt. Accordingly, the present invention establishes a system where one entity stores data in encrypted form, while another independent entity possesses the keys for decrypting the data. This configuration achieves, in essence, a remotely accessible smart card implemented in software, in that the physical possessor of the data has no access to it without a password.

WO 00/79368 A1

**Published:**

— *With international search report.*

— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

# SOFTWARE SMART CARD

## FIELD OF THE INVENTION

The present invention relates to the security of data stored in digital form and, more particularly, relates to security and encryption protocols for preventing unauthorized access to data stored on a computerized database.

## BACKGROUND OF THE INVENTION

A database management system is a collection of computer programs allowing the storage and extraction of information on a database. Database management systems range from small systems running on a personal computer to large systems running on mainframes. Database management systems have a variety of applications, including automated teller systems, flight reservation systems, medical records systems and the like.

Given the sensitive nature of the information discussed above, much effort in the art has been devoted to data security. Data security generally refers to techniques for preventing unauthorized access to data stored on a computer, computerized database, or even a smart card. Many data security techniques involve data encryption and the use of passwords. Data encryption generically refers to methods for translating data into a secret code, called cipher text. To read or gain access to an encrypted file, one must have a secret key or password that enables decryption of the file. As one skilled in the art will recognize, asymmetric encryption (also known as public-key encryption) and symmetric encryption are the two main types of encryption.

Database systems storing data in encrypted form to protect unauthorized access to data are well known in the art. For example, when a user attempts to access a database, the database server prompts the user for a user name and password. If the user is authenticated, he is granted access to the database. Moreover, the files corresponding to an individual user account may be encrypted with a key unique to that account. For example, the key used to encrypt the files may be the result of a salted one-way hash of the password corresponding to the user's account. As is readily apparent to one skilled in the art, a one-way hash function is an algorithm that converts a data collection (such as the contents of a file) into a string of bytes. NIST's Secure Hash Algorithm (SHA) is an example of a one-way hash function (Federal Information Processing Standard (FIPS)

publication 180-1). The resulting string is nearly impossible to invert back to the original file. When the user accesses an account, the password the user inputs is hashed as before and used as a key to decrypt the files stored on the database belonging to that user. However, since users often lose or forget their passwords, a list of passwords or keys must be stored to recover the data. Accordingly, account users must trust the administrators of the database facility not to use their passwords or keys to gain access to their data.

Smart cards offer an alternative way of storing information in encrypted form. A smart card is a small electronic device resembling a credit card. A smart card generally contains memory and an embedded microprocessor and may have a variety of cryptographic protocols and algorithms programmed into it. Smart cards are used in a variety of applications, including, *inter alia*, storing an individual's medical records, passwords, and secret encryption keys. To read from or write to a smart card, the user must insert it into smart card reader. Unlike the remote database discussed above, the stored data remains in the physical possession of the user. Therefore, regardless of the knowledge of others regarding a user's secret password or key, the data stored on the card is only accessible to the physical possessor of the card. One drawback, however, is that, when the smart card is lost, the data stored therein is lost with it.

While the prior art devices fulfill their respective objectives, there exists a need for a new method and system for securely storing data on a remote database that eliminates the trust relationship between account users and the database storage facility. The present invention substantially fulfills this need.

## SUMMARY OF THE INVENTION

The present invention provides methods and systems for preventing unauthorized access to data stored on a computerized database. The present invention contemplates storing data corresponding to individual user accounts in encrypted form. The present invention involves two separate entities to accomplish enhanced data security: a database facility and an escrow facility. The database facility is in physical possession of and administers the database. According to the invention, data corresponding to an individual account is encrypted with a unique cryptographic key. In preferred form, the

cryptographic key is derived from the password corresponding to each account. The database facility, however, has no possession or knowledge of the cryptographic keys used to encrypt the data corresponding to individual user accounts. Rather, after the data is encrypted, the encryption key is transmitted to an escrow facility, which is independent from the database facility. Alternatively, the encryption key is itself encrypted and stored at the database facility in a form that only the escrow facility can readily decrypt. Accordingly, the present invention establishes a system where one entity stores data in encrypted form, while another independent entity possesses the keys for decrypting the data. This configuration achieves, in essence, a remotely accessible smart card implemented in software, in that the physical possessor of the data has no access to it without a password.

As discussed more fully below, the operation of the present invention generally includes three phases: 1) account initialization (establishing a new account); 2) logging in to an existing account; and 3) changing a password to an existing account.

More specifically, the initialization method of the present invention is a protocol for preventing unauthorized access to data stored on a computerized database. The method comprises the steps of (a) receiving a user identification and a password corresponding to the user identification; (b) transforming the password into an encryption key; (c) encrypting, with the key, data corresponding to the user identification; (d) storing the encrypted data in association with the user identification; and (e) encrypting the key for transmission to an escrow facility. In one preferred embodiment, the method comprises (f) transmitting the key to an escrow facility. In addition, other embodiments of the method also comprise the step of (g) storing a second encrypted representation of the key in association with the user identification and the encrypted data, wherein the second encrypted representation results from the application of a one-way hash function to the cryptographic key. In addition, alternative forms of the method feature transmitting an encrypted representation of the key to the escrow facility.

In another preferred embodiment, the initialization method uses a public key provided by the escrow facility to prevent unauthorized access to the user's cryptographic key. This method generally comprises (a) receiving a user identification and a password

corresponding to the user identification; (b) transforming the password into an encryption key; (c) encrypting, with the encryption key, data corresponding to the user identification; (d) storing the encrypted data in association with the user identification; and (e) storing an encrypted representation of the key, wherein the encrypted representation of the key is created by encrypting the key with an asymmetric encryption algorithm according to the public key of the escrow facility.

Yet another preferred embodiment features two layers of encryption. This preferred method comprises the steps of (a) receiving a user identification and a password corresponding to the user identification; (b) transforming the password into a first encryption key; (c) encrypting data corresponding to the user identification with a second encryption key; (d) encrypting, with the first encryption key, the data encrypted according to step (c); (e) storing the data encrypted in step (d) in association with the user identification; and (f) transmitting an encrypted representation of the first encryption key to an escrow facility. In other preferred embodiments, the cryptographic key is encrypted with the escrow facility's public key and stored, rather than being transmitted.

Once a database account has been initialized, it may be accessed in a conventional manner. More specifically, the user provides a user identification corresponding to an account and a password. The password is transformed, as above, to create a cryptographic session key and is used to decrypt the data, which has been encrypted according to one of the methods provided above.

The configuration of the present invention also requires certain unique protocols for changing passwords corresponding to database accounts. As discussed more fully below, the steps involved in a change of password protocol depend on how the database accounts were initialized. In general, however, after a user has been authenticated, a new password is provided. This new password and the data are sent to the escrow facility, which decrypts the data with the old cryptographic key and re-encrypts the data with the new cryptographic key. The re-encrypted data is then transmitted to the database facility for storage.

One preferred method assumes that the escrow facility has possession of the original cryptographic key. This method comprises the steps of (a) receiving a new

password corresponding to a user identification; (b) transforming the new password into a second cryptographic key; (c) transmitting to the escrow facility encrypted data corresponding to the user identification and an encrypted representation of the second cryptographic key; and (d) receiving from the escrow agent the data encrypted according to the new cryptographic key.

Another preferred embodiment corresponds to the situation where the database includes an encrypted representation of the first cryptographic key, where the encrypted representation of the first key is created by the application of an asymmetric encryption algorithm to the first key using a public key of an escrow facility. The method comprises (a) receiving a new password corresponding to a user identification; (b) transforming the new password into a second cryptographic key; (c) transmitting to the escrow facility encrypted data corresponding to the user identification, the encrypted representation of the first cryptographic key, and an encrypted representation of the second cryptographic key; and (d) receiving from the escrow agent the data encrypted according to the second cryptographic key.

Another aspect of the present invention includes the protocols performed by the escrow facility. One such protocol is a method for changing a password corresponding to a user account, the user account having a user identification, the user account including data maintained on a database of a database facility, wherein the data is encrypted with a first cryptographic key, the first cryptographic key being stored by an escrow facility remote from the database. The method comprises the steps of (a) receiving from a database facility and storing an encrypted representation of a first cryptographic key and a designation of a user identification corresponding to the encrypted representation; (b) receiving encrypted data corresponding to the user identification and an encrypted representation of a second cryptographic key, wherein the encrypted data was encrypted with the first cryptographic key; (c) decrypting the encrypted representations of the first cryptographic key and the second cryptographic key; (d) decrypting the encrypted data with the first cryptographic key; (e) encrypting the data, which was decrypted under the step (d), according to the second cryptographic key; and (f) transmitting the data encrypted according to the encrypting step (e) to the database facility.

Another preferred protocol performed by the escrow facility is a method for changing a password corresponding to a user account, the user account including data maintained on a database, wherein the data is encrypted with a first cryptographic key, the database storing an encrypted representation of the first cryptographic key, wherein the encrypted representation of the first key is created by the application of an asymmetric encryption algorithm to the first key using a public key of an escrow facility, the method comprising the steps of (a) receiving from a database facility encrypted data, the encrypted representation of the first cryptographic key, and an encrypted representation of a second cryptographic key, wherein the encrypted data is encrypted with the first cryptographic key; (b) decrypting the encrypted representations of the first cryptographic key and the second cryptographic key; (c) decrypting the encrypted data with the first cryptographic key; (d) encrypting the data, which was decrypted under the step (c), with the second cryptographic key; and (e) transmitting the data encrypted according to the encrypting step (d) to the database facility.

## DEFINITIONS

As used herein, a "database facility" is an entity independent from an escrow facility, discussed below, and stores data in encrypted form. A database facility, according to the present invention, can be a large entity administering a database management system comprising several database servers and managing multiple user accounts. In other embodiments, the "database facility" can be the personal computer of an individual account user.

As used herein, an "escrow facility" is an entity independent from the database facility. According to the present invention, its function is to receive cryptographic keys or cryptographic representations of keys and store them in association with a user identification. In other embodiments, the escrow facility provides a public key to the database facility, as more fully described below. In addition, when called upon, the escrow facility will receive encrypted data corresponding to a user identification and decrypt the data with the cryptographic key corresponding to the user identification.

## DESCRIPTION OF THE DRAWINGS

Figure 1 is a functional block diagram illustrating one embodiment of the system of

the present invention.

Figure 2 is a flowchart diagram showing one preferred method for initializing a database account.

Figure 3 is a flowchart diagram illustrating one preferred method for accessing a secure database account.

Figure 4 is a flowchart diagram illustrating a preferred authentication protocol for use in conjunction with the present invention.

Figure 5 is a flowchart diagram showing a preferred method for changing a password corresponding to a user account.

Figure 6 is a flowchart diagram illustrating a second preferred method for initializing a database account.

Figure 7 is a flowchart diagram showing the protocol for changing a password to an account initialized according to the second preferred embodiment.

Figure 8 is a flowchart diagram illustrating a third preferred method for initializing a user account.

## DETAILED DESCRIPTION OF THE INVENTION

Figure 1 illustrates a preferred embodiment of the present invention as applied to the Internet. Of course, one skilled in the art will readily recognize that the present invention can be applied across any computer network. In other embodiments, communication among account users, database facility 20, and escrow facility 40 can be accomplished over direct (such as dial-up access) or dedicated communications lines, not involving an open computer network.

As Figure 1 illustrates, users access accounts on database facility 20, via client computers 30. As more fully described below, data corresponding to user accounts are stored in database 26 in encrypted form. According to one embodiment of the invention, escrow facility 40 receives encrypted representations of the cryptographic keys used to encrypt the data stored in database 26 of database facility 20. In another embodiment, escrow facility 40 provides a public key for use in an asymmetric (or public-key) encryption algorithm. The database facility uses this public key to store encrypted representations of the cryptographic keys corresponding to user accounts, rather than the

cryptographic keys themselves. In this manner, database facility 20 has no access to the cryptographic keys (without having the escrow facility's private key) and cannot decrypt the data stored in database 26. Similarly, escrow facility 40 has only the cryptographic key and no physical access to associated data.

In one embodiment, database facility 20 includes database servers 22, which receive and process requests submitted by users. Database servers 22 are operably connected to at least one database 26. The database can be any database known in the art. In preferred form, the database is implemented in hardware including a collection of computer programs enabling the storage, modification, and extraction of information on the database. Database hardware may range from personal computers (for small systems) to mainframes (for large systems). Database servers 22 may be implemented in hardware or software, or preferably a combination of both. In preferred form, the server is implemented in computer programs executing on programmable computers each comprising at least one processor, a data storage system (including volatile and non-volatile media), at least one input device, and at least one output device. In one preferred embodiment, database servers 22 are web or Internet servers operably connected to the Internet. In other preferred embodiments, database servers 22 can be directly connected to client computers 30 through dedicated lines.

As Figure 1 shows, the one embodiment of the present invention works in conjunction with a conventional computer having Internet Browsing Software and a connection to the Internet. The user's computer can be any conventional personal computer known in the art. In one preferred embodiment, the user's computer is connected to the Internet via a dial-up connection or through a network line. Such communication could also be wireless. Additionally, suitable Internet browsers for use with the present invention include NETSCAPE NAVIGATOR® or MICROSOFT INTERNET EXPLORER®. The browser implemented on client computer 30 preferably supports the SSL ("Secure Sockets Layer") protocol, the S-HTTP ("Secure HTTP") protocol, or any other similar protocol for transmitting confidential or private information over an open computer network. In one preferred embodiment, communication of passwords and sensitive data, for example, between database facility 20 and client computer 30 employs

the SSL protocol. In operation, a user accesses a database account by launching the browsing software contained in client computer 30 and directs the browser to the web site corresponding to database facility 20. Of course, one skilled in the art will readily recognize that the present invention has application beyond the Internet and the World Wide Web and may be employed on any computer network.

The operation of the present invention generally comprises three phases: 1) account initialization (establishing a new account); 2) logging in to an existing account; and 3) changing a password to an existing account.

Initialization (New Account)

Figure 2 illustrates a first preferred method for initializing a data storage account with the database facility. Database facility 20 receives from client computer 30 a user identification, a password and data to be stored in encrypted form. (Step 100). Database facility then transforms the password to create a cryptographic key that will be used to encrypt the user's data. In one preferred embodiment, a one-way hash function is applied to the inputted password to create the cryptographic key. (Step 102). In preferred form, the password, P, is concatenated with a random or pre-determined string, S, before being operated on by the one-way hash function. Therefore, the cryptographic key is represented by $K = H(P + S)$, where H represents the one-way hash function. (See Figure 2.) Suitable one-way hash functions include, but are not limited to, MD4, MD5, SHA, Snefru and the like. In yet other embodiments, the one-way hash function can be performed on client computer 30 and subsequently transmitted to database server 22 over a secure communications protocol, such as SSL.

Digital data, D, is received at server 22 and then encrypted with the cryptographic key, K, derived in step 102 and stored in database 26 of database facility 20 in association with the user identification. Suitable encryption algorithms include symmetric algorithms, such as DES, 3DES or RC4, and asymmetric or public-key algorithms, such as RSA or ElGamal. In addition, the random string, S, is stored in the database alongside the hashed password, so that $H(P+S)$ can be re-computed from P and S when the user logs in. As one skilled in the art will recognize, the use of S is optional; however, it is customary in the art to include S in order to impede dictionary attacks against the password.

In an alternative embodiment, client computer 30 receives the cryptographic key, K, from server 22 using a secure communications protocol, encrypts data with the key, and transmits the encrypted data to server 22 for storage on database 26. The cryptographic key, K, is then transmitted to escrow facility 40.

In one preferred embodiment, the database facility stores user accounts in database 26 as a series of records, each record including a field for the user identification, UserID, the encrypted data K(D). Optionally, a second one-way hash function, H, can be applied to the cryptographic key, K, of step 102 and stored in the same record as the encrypted data, K(D) and the user identification, UserID. The results of this second hashing, H(K), can be used to authenticate a user at login (described more fully below).

In other embodiments of the present invention, rather than encrypting the user's files directly with a key derived from the password, the user's files are encrypted with a random key created when the account is first created. This random key is encrypted by the user's password (or a key derived from the user's password) and the encrypted key is stored in the database. The password-derived key is then transmitted to the escrow facility and stored. Therefore, if the user's password changes, only one record in the database needs to be updated. This is preferable to using the password directly if the amount of user data requiring encryption is large. Under this embodiment, the encrypted key is transmitted to the escrow facility, which decrypts the key with the user's password and transmits it back to the database facility or the user.

In one preferred form, the cryptographic key is then transmitted to escrow facility 40, which stores the cryptographic key in association with a user identification. (*See* Figure 2, step 106.) The cryptographic key may be transmitted by database facility 20 or client computer 30. In other preferred embodiments, the cryptographic key is encrypted using the escrow facility's public key and stored either at database facility 20 or locally at client computer 30. *See* Figure 6, step 508. However, according to the protocols of the present invention, in no event is database facility 20 to store the cryptographic keys, which are used to encrypt account data, in unencrypted form or in an encrypted form invertible by the database facility, when the user is not logged in.

As to the protocol where the cryptographic key is transmitted to escrow facility 40,

many variations are possible. For example, the cryptographic key can be further encrypted using a public key of the escrow facility and then transmitted in association with the corresponding user identification, or an encrypted representation thereof. Furthermore, the cryptographic key can be encrypted and transmitted by a secure processor. The secure processor can encrypt the key using a symmetric or asymmetric encryption algorithm with a secret key known by escrow facility 40. A secure cryptographic processor is a hardware device that performs cryptographic operations (encryption, decryption, etc.) using a stored internal key. The device is designed to perform these operations only in strict accordance with a programmed security policy (such as, restrict use of certain keys to certain users) and to resist attempts to circumvent the policy or extract the key, including by physical means such as dismantling the hardware or probing it with electronic instruments. An example of a secure processor is the NFast/CA Cryptographic Accelerator made by NCipher Corp. (http://www.ncipher.com). There is a set of US federal standards (FIPS 140-1, http://csrc.nist.gov/cryptval) describing levels of physical attack resistance for which these devices can be designed. The NFast/CA Cryptographic Accelerator is certified at FIPS 140-1 level 3. The features of the secure processor must include the capability of storing secret keys in a manner that: 1) the secret key cannot be extracted from the processor, except possibly by defeating the processor's security features; 2) the secret key can be tagged inside the processor as being useable to encrypt data but not to decrypt it (so that decryption requests will be refused). Furthermore, the same secret key in the secure processor must be embedded in the escrow facility's system (either in another secure processor or in software) in a way that it is capable of decryption. In this manner, the system combines the high speed and compact key representation of secret key systems with the one-way encryption capability of public key systems. Public key systems provide one-way encryption capability because of the mathematical difficulty of inverting the public key function. The secure processor provides one-way encryption because of the physical difficulty of getting the secret key out of the secure processor.

As discussed above, Figure 6 illustrates another preferred embodiment of the present invention. The second preferred embodiment differs from the first preferred

initialization protocol in that the password derived key is encrypted with an asymmetric (or public key) algorithm using a public key, PK, of the escrow facility and stored at the database facility rather than being transmitted. (See Figure 6, step 508). Accordingly, without the escrow facility's private key, storage facility or anyone else in physical possession of the user's data has no way to decrypt it and thereby gain access. As discussed below, the encrypted representation of the key and the data encrypted with this key is transmitted to the escrow facility during execution of a password change.

In yet another embodiment (See Figure 8), account data passes through two layers of encryption. More specifically, data (D) corresponding to a particular user's account is first encrypted using the secret key (SK) of storage facility 20. (Step 706). The encrypted data, SK(D) is then encrypted using the password-derived key, K, of step 704. Because the data is first encrypted using the secret key of storage facility 20, escrow facility 40 has no meaningful access to the data, when it is sent the data during a password change protocol (discussed more fully below). As one skilled in the art will recognize, the encryption step 706 can be performed using a symmetric encryption algorithm with a secret key or an asymmetric encryption algorithm using a public key for encryption and the private key for decryption. Of course, this extra layer of encryption requires the user's data to be decrypted a second time before a user can access the data.

Login to Existing Account

Figures 3 and 4 show a preferred method whereby a user gains access to an existing account. As is conventional, a user logs in to an account by accessing database server 22 and, when prompted, provides a user identification or user name (UserID) and a password (P). (See Figure 3, step 202 and Figure 4, step 302). The user is authenticated, in one preferred embodiment, according to the method illustrated in Figure 4. Namely, the inputted password is concatenated with the same random string, S, generated in step 102 of Figure 2 and hashed twice, [C = H(H(P+S))]. The resulting value is compared to the value of H(K) stored in the record corresponding to the user's account (See Figure 2, step 104). If C = H(K), then the user is authentic (step 306) and is granted access to the account. A session key, $K_s$, is derived from a single hash of the user's salted password and used by server 22 to decrypt the data stored in the user's

account (See Figure 3, steps 206 and 208). Once a user has gained access to his or her account, the user may read the data or change the data. At logout or, optionally, before logout, the changed data is re-encrypted using $K_c$ and stored in database 26. $K_c$ is erased from database server 22 at logout as well. As discussed above, communication of data between database facility 20 and client computer 30 is preferably conducted using a security protocol, like SSL or S-HTTP. In other embodiments, after authentication, database 22 server transmits both the encrypted data and the key to client computer 30, again preferably using a secure communications protocol (SSL, S-HTTP, or the like). Under this embodiment, client computer 30 decrypts the data using the key derived at login.

Furthermore, as alluded to above, if a user account was initialized according to the protocol illustrated in Figure 8, then the user's data must be further decrypted using the secret key of the storage facility.

Change Password to Existing Account

Figure 5 provides a protocol for changing passwords corresponding to accounts that have been initialized according to the steps outlined in Figure 2. A password change occurs either because the user desires a new password or has lost or forgotten the existing password. In the first case, a user simply enters the old password and indicates that a password change is desired and enters the new password, as is conventional. In the second case, the user must contact the administrators of the database facility who authenticate the user by criteria other than the old password. How this authentication is accomplished is not critical to the present invention. Any conventional method may be used. According to the invention, a new cryptographic key is created in either case.

More specifically, in response to a request for a change of the password to an account, database server 22 receives the user identification corresponding to a particular account and a new password (step 402). The new password is hashed to create a new cryptographic key (step 404). In step 406, the user's data and the new key are sent to the escrow facility 40. Escrow facility 40 decrypts the data with the old cryptographic key it received according to step 106 of Figure 2 and re-encrypts the data with the new cryptographic key (step 408). Escrow facility 40 stores the new key in association with the

user identification corresponding to the account data and transmits the encrypted data to the storage facility 20, where the user can again access the data as provided above.

In addition, Figure 7 illustrates a preferred protocol for changing the password to accounts that have been initialized according to the steps outlined in Figure 6. Step 606 involves transmitting, to the escrow facility, the previous cryptographic key encrypted with the escrow facility's public key, the data encrypted according to the previous key, and an encrypted representation of the new key. As with the protocol of Figure 6, escrow facility decrypts the data with the previous key and re-encrypts the data with the new key (step 608). Escrow facility 40 then transmits the encrypted data to storage facility 20 and deletes both the old and new cryptographic keys. Storage facility 20 stores an encrypted representation of the new cryptographic key in association with the encrypted data and corresponding user identification. As with the initialization protocol, the encrypted representation of the new cryptographic key is generated by applying an asymmetric encryption algorithm to the cryptographic key using a public key of escrow facility 40. Otherwise, the change of password protocol according to Figure 7 is essentially the same as the protocol outlined in Figure 6.

As one skilled in the art will recognize, during the password change protocols described above, escrow facility has access to the user's data. The preferred protocol of Figure 8 includes an additional data encryption step (step 706) and such access. More specifically, since the data is encrypted with a secret key provided by database facility 20, escrow facility has no access to the data when it receives it for decryption with the old key and re-encryption with the new key.

## SUMMARY

With respect to the above-provided description, one skilled in the art will readily recognize that the present invention has application in a variety of contexts. The foregoing description illustrates the principles of the present invention and provides examples of its implementation. For example, although the preferred embodiment is described as working in conjunction with an Internet browser, the present invention may be used in connection with any suitable software application for accessing files throughout a computer network. Accordingly, the above-provided description is not intended to limit the scope of the claims to the exact embodiments shown and described.

CLAIMS

1. A method for preventing unauthorized access to data stored on a computerized database, said method comprising the steps of

(a) receiving a user identification and a password corresponding to said user identification;

(b) transforming said password into an encryption key;

(c) encrypting, with said key, data corresponding to said user identification;

(d) storing said encrypted data in association with said user identification; and

(e) transmitting said key to an escrow facility.

2. The method of claim 1 further comprising the step of

(f) storing an encrypted representation of said key in association with said user identification and said encrypted data, wherein said encrypted representation results from the application of a one-way hash function to said key.

3. The method of claim 1 wherein said transforming step (b) is performed by hashing said password to create an encryption key.

4. The method according to claim 1 wherein said transforming step (b) further comprises

(b1) adding additional characters to said password to create a salted password; and

(b2) hashing said salted password to create an encryption key.

5. The method of claim 2 wherein said transmitting step (e) is performed using a secure communications protocol.

6. The method of claim 5 wherein said secure communications protocol is one selected from the group consisting of SSL and S-HTTP.

7. The method of claim 1 wherein step (c) is performed at a server and said encrypted data is stored in a database connected to said server.

8. A method for preventing unauthorized access to data stored on a computerized database, said method comprising the steps of

(a) receiving a user identification and a password corresponding to said user identification;

(b) transforming said password into an encryption key;

(c) encrypting, with said key, data corresponding to said user identification;

(d) storing said encrypted data in association with said user identification; and

(e) encrypting said key for transmission to an escrow facility.

9. The method of claim 8 further comprising the step of

(f) transmitting said key to said escrow facility.

10. The method of claim 8 further comprising the step of

(g) storing an encrypted representation of said key in association with said user identification and said encrypted data, wherein said encrypted representation results from the application of a one-way hash function to said key.

11. The method of claim 8 wherein said transforming step (b) is performed by hashing said password to create an encryption key.

12. The method of claim 8 wherein said transforming step (b) further comprises

(b1) adding additional characters to said password to create a salted password; and

(b2) hashing said salted password to create an encryption key.

13. The method of claim 9 wherein said transmitting step (f) is performed using a secure communications protocol.

14. The method of claim 13 wherein said secure communications protocol is one selected from the group consisting of SSL and S-HTTP.

15. A method for preventing unauthorized access to data stored on a computerized database, said method comprising the steps of

(a) receiving a user identification and a password corresponding to said user identification;

(b) transforming said password into an encryption key;

(c) encrypting, with said key, data corresponding to said user identification;

(d) storing said encrypted data in association with said user identification; and

(e) transmitting an encrypted representation of said key to an escrow facility.

16. The method of claim 15 further comprising the step of

(f) storing a second encrypted representation of said key in association with said user identification and said encrypted data, wherein said second encrypted representation results from the application of a one-way hash function to said key.

17. The method of claim 15 wherein said transforming step (b) further comprises

(b1) adding additional characters to said password to create a salted password; and

(b2) hashing said salted password to create an encryption key.

18. The method of claim 15 wherein said escrow facility has a public key, and wherein said encrypted representation of said key is created with an asymmetric encryption algorithm using the public key of said escrow facility.

19. The method of claim 15 wherein said encrypted representation of said key is performed by a secure processor and wherein said secure processor performs said transmitting step (e).

20. The method of claim 15 wherein said transmitting step (e) further includes transmitting an encrypted representation of said user identification to said escrow facility.

21. A method for preventing unauthorized access to data stored on a computerized database, wherein a user stores information in encrypted form on the database of a database facility, and wherein an independent escrow facility possesses at least one public key, said method comprising the steps of

(a) receiving a user identification and a password corresponding to said user identification;

(b) transforming said password into an encryption key;

(c) encrypting, with said encryption key, data corresponding to said user identification;

(d) storing said encrypted data in association with said user identification;

(e) storing an encrypted representation of said key, wherein said encrypted representation of said key is created by encrypting said key with an asymmetric encryption algorithm according to said public key of said escrow facility.

22. The method of claim 21 further comprising the step of

(f) storing a second encrypted representation of said key in association with said user identification and said encrypted data, wherein said second encrypted representation results from the application of a one-way hash function to said key.

23. The method of claim 21 wherein said transforming step (b) further comprises

(b1) adding additional characters to said password to create a salted password; and

(b2) hashing said salted password to create an encryption key.

24. A method for preventing unauthorized access to data stored on a computerized database, said method comprising the steps of

(a) receiving a user identification and a password corresponding to said user

identification;

(b) transforming said password into a first encryption key;

(c) encrypting data corresponding to said user identification with a second encryption key;

(d) encrypting, with said first encryption key, said data encrypted according to step (c);

(e) storing said data encrypted in step (d) in association with said user identification; and

(f) transmitting an encrypted representation of said first encryption key to an escrow facility.

25. The method of claim 24 further comprising the step of

(g) storing a second encrypted representation of said key in association with said user identification and said encrypted data, wherein said second encrypted representation results from the application of a one-way hash function to said key.

26. The method of claim 24 wherein said transforming step (b) further comprises

(b1) adding additional characters to said password to create a salted password; and

(b2) hashing said salted password to create an encryption key.

27. The method of claim 24 wherein said escrow facility has a public key, and wherein said encrypted representation of said key is created with an asymmetric encryption algorithm using the public key of said escrow facility.

28. The method of claim 24 wherein said encrypted representation of said key is performed by a secure processor and wherein said secure processor performs said transmitting step (f).

29. The method of claim 24 wherein said transmitting step (f) further includes

transmitting an encrypted representation of said user identification to said escrow facility.

30. A method for preventing unauthorized access to data stored on a computerized database, said method comprising the steps of

(a) receiving a user identification and a password corresponding to said user identification;

(b) transforming said password into a first encryption key;

(c) encrypting data corresponding to said user identification with a second encryption key;

(d) encrypting, with said first encryption key, said data encrypted according to step (c);

(e) storing said data encrypted in step (d) in association with said user identification; and

(f) storing an encrypted representation of said first encryption key, wherein said encrypted representation of said key is created by encrypting said key with an asymmetric encryption algorithm according to said public key of said escrow facility.

31. The method of claim 30 further comprising the step of

(g) storing a second encrypted representation of said key in association with said user identification and said encrypted data, wherein said second encrypted representation is the result of the application of a one-way hash function to said key.

32. The method of claim 30 wherein said transforming step (b) further comprises

(b1) adding additional characters to said password to create a salted password; and

(b2) hashing said salted password to create a first encryption key.

33. A method for preventing unauthorized access to data stored on a computerized database, said method comprising the steps of

(a) receiving a user identification and a password corresponding to said user

identification;

(b) transforming said password into a first encryption key;

(c) encrypting, with a second encryption key, data corresponding to said user identification;

(d) encrypting said second encryption key with said first encryption key to create an encrypted representation of said second encryption key;

(d) storing said encrypted data and said encrypted representation of second encryption key in association with said user identification; and

(e) encrypting said first encryption key for transmission to an escrow facility.

34. The method of claim 33 wherein said second encryption key is randomly generated.

35. The method of claim 33 further comprising the step of

(f) transmitting said first encryption key, encrypted according to step (e), to said escrow facility.

36. The method of claim 33 wherein said transforming step (b) further comprises

(b1) adding additional characters to said password to create a salted password; and

(b2) hashing said salted password to create a first encryption key.

37. The method of claim 33 wherein said encrypting step (e) is performed with an asymmetric encryption algorithm according to a public key of said escrow facility.

38. The method of claim 35 wherein said encrypting step (e) is performed with an asymmetric encryption algorithm according to a public key of said escrow facility.

39. A method for changing a password corresponding to a user account, said user account having a user identification, said user account including data maintained on a database, wherein said data is encrypted with a first cryptographic key, said first

cryptographic key being stored by an escrow facility remote from said database, said method comprising the steps of

(a) receiving a new password corresponding to a user identification;

(b) transforming said new password into a second cryptographic key;

(c) transmitting to said escrow facility encrypted data corresponding to said user identification and an encrypted representation of said second cryptographic key,

(d) receiving from said escrow agent said data encrypted according to said new cryptographic key.

40. The method of claim 39 further comprising the step of

(e) storing a second encrypted representation of said second cryptographic key in association with said user identification and said encrypted data, wherein said second encrypted representation results from the application of a one-way hash function to said second key.

41. The method of claim 39 wherein said transforming step (b) further comprises

(b1) adding additional characters to said password to create a salted password; and

(b2) hashing said salted password to create an encryption key.

42. The method of claim 39 wherein said escrow facility has a public key, and wherein said encrypted representation of said second key is created with an asymmetric encryption algorithm using the public key of said escrow facility.

43. The method of claim 39 wherein said encrypted representation of said second key is performed by a secure processor and wherein said secure processor performs said transmitting step (c).

44. The method of claim 39 wherein said transmitting step (c) further includes transmitting an encrypted representation of said user identification to said escrow facility.

45. A method for changing a password corresponding to a user account, said user account including data maintained on a database, wherein said data is encrypted with a first cryptographic key, said database storing an encrypted representation of said first cryptographic key, wherein said encrypted representation of said first key is created by the application of an asymmetric encryption algorithm to said first key using a public key of an escrow facility, said method comprising the steps of

(a) receiving a new password corresponding to a user identification;

(b) transforming said new password into a second cryptographic key;

(c) transmitting to said escrow facility encrypted data corresponding to said user identification, said encrypted representation of said first cryptographic key, and an encrypted representation of said second cryptographic key; and

(d) receiving from said escrow agent said data encrypted according to said second cryptographic key.

46. The method of claim 45 further comprising the step of

(e) storing a second encrypted representation of said second key in association with said user identification and said encrypted data, wherein said second encrypted representation results from the application of a one-way hash function to said key.

47. The method of claim 45 wherein said transforming step (b) further comprises

(b1) adding additional characters to said password to create a salted password; and

(b2) hashing said salted password to create an encryption key.

48. The method of claim 45 wherein said escrow facility has a public key, and wherein said encrypted representation of said second key is created with an asymmetric encryption algorithm using the public key of said escrow facility.

49. The method of claim 45 wherein said encrypted representation of said second key is performed by a secure processor and wherein said secure processor performs said

transmitting step (c).

50. The method of claim 45 wherein said transmitting step (c) further includes transmitting an encrypted representation of said user identification to said database facility.

51. A method for changing a password corresponding to a user account, said user account having a user identification, said user account including data maintained on a database of a database facility, wherein said data is encrypted with a first cryptographic key, said first cryptographic key being stored by an escrow facility remote from said database, said method comprising the steps of

(a) receiving from a database facility and storing an encrypted representation of a first cryptographic key and a designation of a user identification corresponding to said encrypted representation;

(b) receiving encrypted data corresponding to said user identification and an encrypted representation of a second cryptographic key, wherein said encrypted data was encrypted with said first cryptographic key;

(c) decrypting said encrypted representations of said first cryptographic key and said second cryptographic key;

(d) decrypting said encrypted data with said first cryptographic key;

(e) encrypting said data, which was decrypted under said step (d), according to said second cryptographic key;

(f) transmitting said data encrypted according to said encrypting step (e) to said database facility.

52. The method of claim 51 wherein said encrypted representation of said first cryptographic key was created with an asymmetric encryption algorithm using a public key of said escrow facility; and wherein said decrypting step (c) is performed with a private key of said escrow facility.

53. The method of claim 51 wherein said encrypted representation of said second cryptographic key was created with an asymmetric encryption algorithm using a public key of said escrow facility; and wherein said decrypting step (c) is performed with a private key of said escrow facility.

54. A method for changing a password corresponding to a user account, said user account including data maintained on a database, wherein said data is encrypted with a first cryptographic key, said database storing an encrypted representation of said first cryptographic key, wherein said encrypted representation of said first key is created by the application of an asymmetric encryption algorithm to said first key using a public key of an escrow facility, said method comprising the steps of

(a) receiving from a database facility encrypted data, said encrypted representation of said first cryptographic key, and an encrypted representation of a second cryptographic key, wherein said encrypted data is encrypted with said first cryptographic key;

(b) decrypting said encrypted representations of said first cryptographic key and said second cryptographic key;

(c) decrypting said encrypted data with said first cryptographic key;

(d) encrypting said data, which was decrypted under said step (c), with said second cryptographic key;

(e) transmitting said data encrypted according to said encrypting step (d) to said database facility.

55. The method of claim 54 wherein said encrypted representation of said second cryptographic key was created with an asymmetric encryption algorithm using a public key of said escrow facility; and wherein said decrypting step (c) is performed with a private key of said escrow facility.

56. A method for changing a password corresponding to a user account, said user account including data maintained on a database, wherein said data is encrypted with a first cryptographic key, said database storing an encrypted representation of said first

cryptographic key, wherein said encrypted representation of said first key is created by encrypting said first cryptographic key with a second cryptographic key, said method comprising the steps of

(a) receiving from a database facility said encrypted representation of said first cryptographic key and an encrypted representation of a second cryptographic key;

(b) decrypting said encrypted representation of said second cryptographic key;

(c) decrypting said encrypted representation of said first cryptographic key with said second cryptographic key;

(d) transmitting said first cryptographic key to said database facility.

57. The method of claim 56 wherein said encrypted representation of said second cryptographic key is created from the application of an asymmetric encryption algorithm using a public key of said escrow facility; and wherein said decrypting step (b) is performed with the corresponding private key of said escrow facility.

58. A method for preventing unauthorized access to data stored on a computerized database, said database operably connected to a server, said server operably connected to a computer network, said computer network further comprising at least one client computer and at least one escrow facility operably connected to said computer network, said method comprising the steps of

(a) receiving, at said server, a user identification and a password corresponding to said user identification;

(b) transforming, at said server, said password into an encryption key;

(c) encrypting at said server, with said key, data corresponding to said user identification;

(d) storing said encrypted data in association with said user identification on said database; and

(e) transmitting said key to said escrow facility.

59. The method of claim 58 further comprising the step of receiving at said server data

from said client computer.

60. The method of claim 59 wherein said receiving data step is conducted using a secure communications protocol.

61. A method for preventing unauthorized access to data stored on a computerized database, the method comprising the steps of

(a) receiving, at a server, a user identification and a password from a client computer;

(b) transforming, at said server, said password into a cryptographic key;

(c) decrypting, at said server, data corresponding to said user identification with said cryptographic key; and

(d) transmitting said data to said client computer.

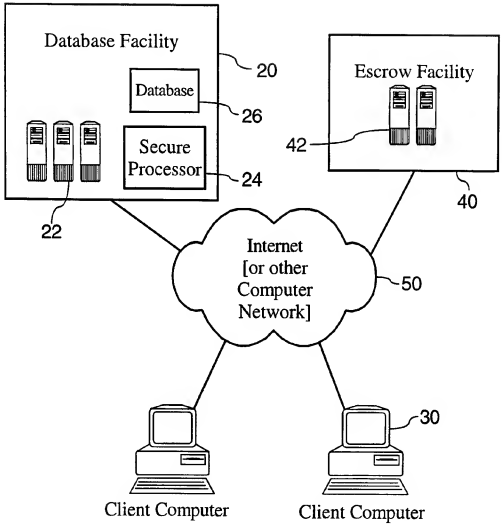

Database Facility
20
Database
26
Secure Processor
24
22
Escrow Facility
42
40
Internet [or other Computer Network]
50
30
Client Computer
Client Computer

FIG. 1

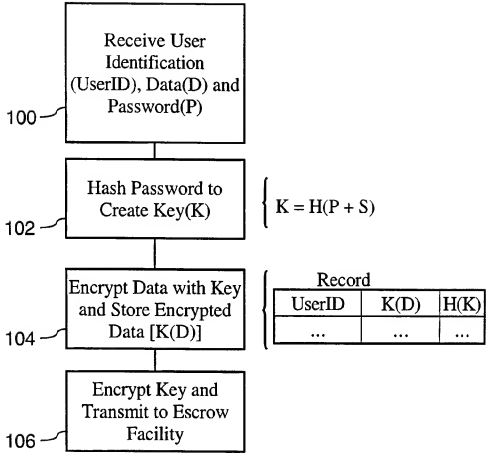

Receive User Identification (UserID), Data(D) and Password(P)
100
Hash Password to Create Key(K)
102
K = H(P + S)
Encrypt Data with Key and Store Encrypted Data [K(D)]
104
Record
UserID
K(D)
H(K)
...
...
...
Encrypt Key and Transmit to Escrow Facility
106

FIG. 2

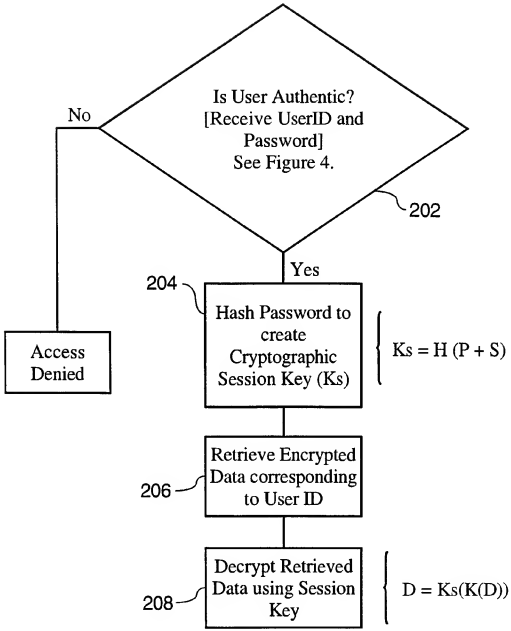

Is User Authentic?
[Receive UserID and Password]
See Figure 4.
202
No
Yes
Access Denied
204
Hash Password to create Cryptographic Session Key (Ks)
Ks = H (P + S)
206
Retrieve Encrypted Data corresponding to User ID
208
Decrypt Retrieved Data using Session Key
D = Ks(K(D))

FIG. 3

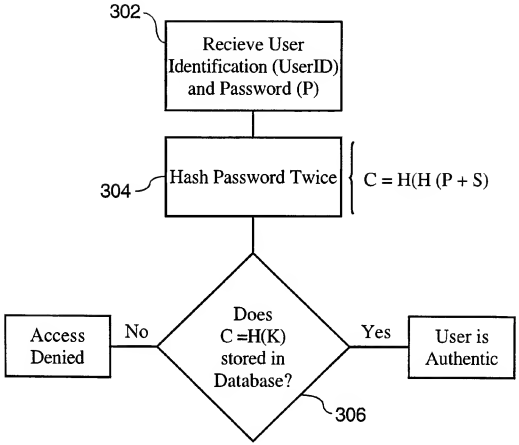

302
Recieve User Identification (UserID) and Password (P)
304
Hash Password Twice
C = H(H (P + S)
Does C =H(K) stored in Database?
306
No
Access Denied
Yes
User is Authentic

FIG. 4

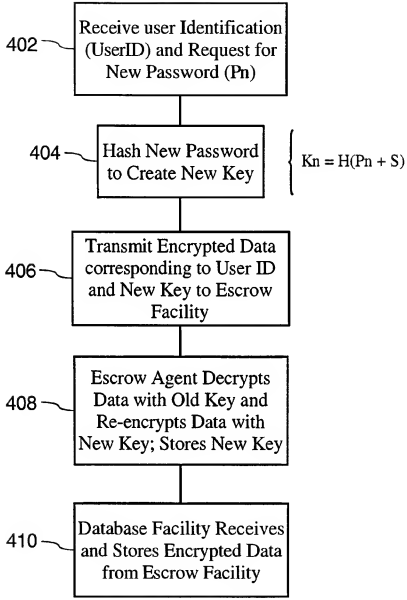

402
Receive user Identification (UserID) and Request for New Password (Pn)
404
Hash New Password to Create New Key
Kn = H(Pn + S)
406
Transmit Encrypted Data corresponding to User ID and New Key to Escrow Facility
408
Escrow Agent Decrypts Data with Old Key and Re-encrypts Data with New Key; Stores New Key
410
Database Facility Receives and Stores Encrypted Data from Escrow Facility

FIG. 5

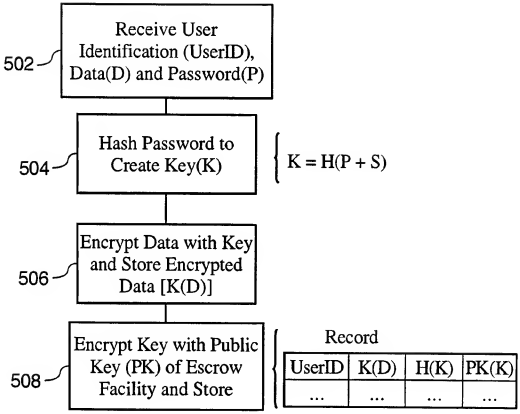

Receive User Identification (UserID), Data(D) and Password(P)
502
Hash Password to Create Key(K)
504
K = H(P + S)
Encrypt Data with Key and Store Encrypted Data [K(D)]
506
Encrypt Key with Public Key (PK) of Escrow Facility and Store
508
Record
UserID
K(D)
H(K)
PK(K)
...
...
...
...

FIG. 6

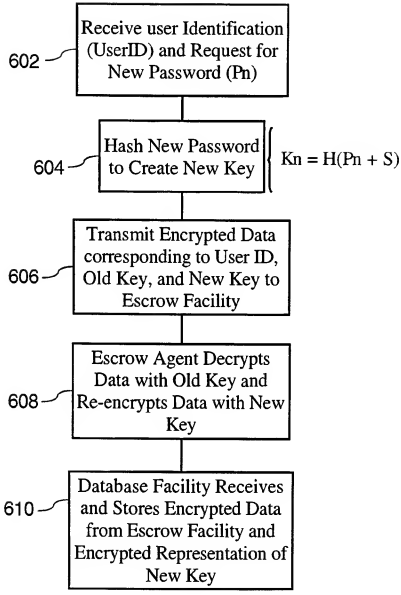

602
Receive user Identification (UserID) and Request for New Password (Pn)
604
Hash New Password to Create New Key
Kn = H(Pn + S)
606
Transmit Encrypted Data corresponding to User ID, Old Key, and New Key to Escrow Facility
608
Escrow Agent Decrypts Data with Old Key and Re-encrypts Data with New Key
610
Database Facility Receives and Stores Encrypted Data from Escrow Facility and Encrypted Representation of New Key

FIG. 7

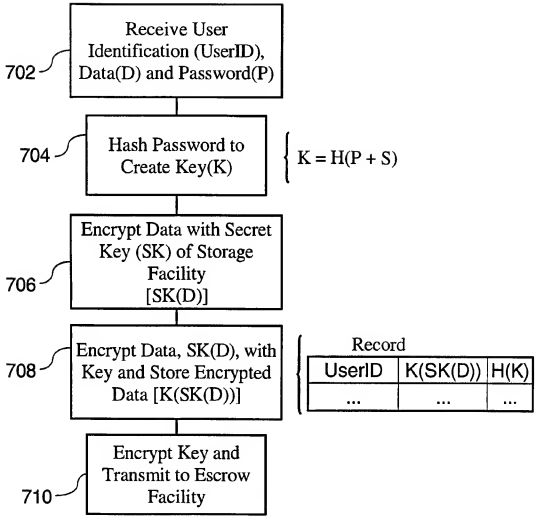

Receive User Identification (UserID), Data(D) and Password(P)
702
Hash Password to Create Key(K)
704
K = H(P + S)
Encrypt Data with Secret Key (SK) of Storage Facility [SK(D)]
706
Encrypt Data, SK(D), with Key and Store Encrypted Data [K(SK(D))]
708
Record
UserID
K(SK(D))
H(K)
...
...
...
Encrypt Key and Transmit to Escrow Facility
710

FIG. 8